Introduction

Girl Security, a nonpartisan, non-profit organization building equitable pathways in national security for girls, women, and gender minorities, is proud to share the inaugural National Girl Security Strategy - an assessment of national security through the lens of twenty-six fellows ages 15 through 20 from across the United States.

The U.S. Government's National Security Strategy should serve as a guide to Congress, as well as the American public and global community, to better understand a particular presidential administration's strategic priorities. The strategy should also provide some detail and depth as to how a particular administration may implement its respective priorities. Often, however, the National Security Strategy remains unfamiliar to most Americans on behalf of whom these crucial decisions are made and actions are taken, despite the lasting and pervasive impacts. This document is intended to provide a dedicated space for girls, women, and gender minorities - those historically underrepresented in national security and often overlooked in national security priorities and pathways - to add their unparalleled insights to discourse around the nation and the world's most pressing security challenges.

As we say at Girl Security, girls and women are taught to fear everything and often secured from nothing. They are the most innately qualified security practitioners, yet the American public and a global community are often deprived of the opportunity to see "security" through their lenses. To create this strategy, fellows were provided a set of themes that represent current national security challenges including: artificial intelligence, climate security, gender-based violence, cybersecurity, nuclear weapons, and domestic terrorism. In cohorts of five, the fellows spent fifteen weeks implementing a research strategy that included informational interviews with leading experts. As the reader will find, each collaborative approached their strategy differently: some took a more granular approach to a particular action or population and others focused their analysis on holistic efforts. Overall, this strategy includes actionable recommendations to bridge the generational gaps in understanding of national security, informed by girls’ and women's lived experiences. In addition, each cohort opted for an intersectional approach to the recommendations.

Girl Security is committed to advancing the occupational identity of girls, women, and gender minorities in national security pathways, as well as efforts to reform those cultures, policies, and practices which have resulted in the exclusion of these same populations.
Girl Security’s mission is guided by a principled belief that continuing to undervalue more than half the population in the most powerful political realm in the world will impede America’s ability to remain agile in a global security landscape, and more importantly, its ability to secure the fundamental democratic values upon which America was founded. Civic empowerment is a core motivating purpose of our work.

At Girl Security, we believe in creating a safe and supportive space for participants to explore and test the boundaries of their own understanding of fundamentally complex issues. We are working to shift norms by supporting the advancement and amplification of girls’ and women’s ideas in a most important domain. Our emphasis on such competencies as ethical decision making, strategy and implementation, and critical thinking equip participants with enduring, transferable skills across professional pathways.

National security is the most important common cause: our continued national security will rely on our nation's ability to forge a new, common understanding of the democratic ideals valued by all and required to preserve the future of American democracy and global security.

Girl Security would like to thank Erin Connolly for her leadership, guidance, and commitment to empowering future generations of national security leaders, while also serving her country. We would also like to thank Girl Security mentors, mentees, supporters, allies, and champions for their dedication to building a national security workforce for the future. Thank you to El Nicklin for her creative direction.

On behalf of the Girl Security Team, we want to thank and congratulate the Fellows for their commitment to this work amid such uncertain times.

Lauren Bean Buitta
Founder & CEO
Girl Security
# Table of Contents

**Girl Security Introduction**

**A. ADVANCING A MORE INCLUSIVE APPROACH TO CLIMATE SECURITY**
Alyssa Eamranond (Age: 19), Ilinca Drondoe (Age: 17), Jasmine De Leon (Age: 18), Kelly Huang (Age: 18), Nicole Chowdhury (Age: 16), and Prachi Gyanmote (Age: 17)

**B. PROMOTING A WHOLE-OF-SOCIETY APPROACH TO CYBERSECURITY**
Amanda Kay (Age: 17), Amulya Panakam (Age: 17), Sarah Velez (Age: 18), Sravya Kotamrajju (Age: 16), and Zayna Cheema (Age: 15)

**C. ACKNOWLEDGING THE PERVERSIVE IMPACTS OF GENDER-BASED VIOLENCE ON NATIONAL SECURITY**
Abby Tupper (Age: 17), Ashika Srivastava (Age: 18), Gurman Dhaliwal (Age: 19), Kenatu Habetaslassa (Age: 19), and Zikora Akanegbu (Age: 16)

**D. CONFRONTING THE RISE OF DOMESTIC TERRORISM**
Aimee Yan (Age: 19), Alexandra Rozmarin (Age: 17), Megan Mingo (Age: 19), Rachel Rochford (Age: 16), and Razel Suansing (Age: 19)

**E. ADVANCING A MORE ETHICAL APPROACH TO ARTIFICIAL INTELLIGENCE AND NUCLEAR WEAPONS**
Ava Luna Pardo-Keegan (Age: 19), Ilyne Castellanos (Age: 20), Kristie Moore, (Age: 18), Mary Raines Alexander (Age: 17), and Sama Kubba (Age: 18)

**F. Endnotes**
A. ADVANCING A MORE INCLUSIVE APPROACH TO CLIMATE SECURITY

“The policy recommendations below emphasize the intersectionality of environmental protection, defense and national security, and social justice and equality.”

Alyssa Eamranond (Age: 19), Ilinca Drondoe (Age:17), Jasmine De Leon (Age: 18), Kelly Huang (Age: 18), Nicole Chowdhury (Age: 16), and Prachi Gyanmote (Age: 17)

Climate change presents a crucial threat to U.S. national security. As a “threat multiplier,” it exacerbates existing national security challenges such as natural disasters, resource scarcity, economic disruptions, mass displacement, and global-power rivalries. A United States strategy to address climate change requires individual action and advocacy at the local level as well as broader change on the national level to mitigate climate change and prepare for its effects.

The implications of climate change on national and international security are multifold. As countries contend with the pressure to accelerate the reduction of greenhouse gas emissions, geopolitical tensions are forecasted to escalate. Increased drought and natural disasters cause food and water shortages and intensify conflict within and between nations over access to vital resources. Geopolitical flashpoints will be exacerbated by mass displacement due to climate change impacts, which may lead to unrest as well as terrorist recruitment from vulnerable populations. Furthermore, developing nations are disproportionately impacted by the changing climate in addition to being the least able to adapt to such changes. All of these factors will further threaten national security priorities, while resulting in greater U.S. involvement in humanitarian aid and stabilization efforts.

With respect to defense, the Pentagon’s October 2021 report on the impacts of climate change states that the environmental crisis is affecting U.S. military installations and service members, while increasing the number of missions conducted by the Department of Defense. Climate change also induces sea-level rise, storm surges, and flooding that are likely to cause infrastructure damage, loss of utilities, and loss of operational capability for defense operations; a sea-level rise of three feet would threaten 128 DoD bases.

The many implications of climate change are poised to affect nearly all Americans and its allies; thus, addressing the impacts of the climate crisis is vital when it comes to ensuring security and future prosperity for both the United States and the world at large. Therefore, the United States must concurrently work to prevent further climate change and adapt to its inevitable consequences. This requires setting targets for long-term reductions in
carbon emissions and collaborating with the international community to plan for the destabilizing effects of natural disasters. Furthermore, a strategy should ensure that those most affected by these impacts (i.e., women, especially women of color) are given a voice at the table during policymaking and strategizing for improved climate security. The objective of this climate security strategy is to promote policies guided by values of resilience, equity, safety, and inclusivity. The policy recommendations provided in this document are sectioned into four key areas: education, whole-of-government approach, elevating marginalized communities, and allocation of resources.

The Current State of Climate Security
It is vital to understand the current state of climate security to properly diagnose U.S. resource allocation and policy changes. Climate change is a macro- and micro-level issue. Individual communities and groups including women, minority, and Native and indigenous communities are adversely impacted through actions like deforestation, globalization, and barriers to education. This has resulted in greater malnutrition, food insecurity, and less biodiversity, while also widening detrimental gaps between those nations that have the resources to implement climate security measures and those that do not.

"Dynamics in the national and international security space such as the COVID-19 pandemic, 'great power' competition with other nation states, and the rise of domestic terrorism, as well as the spread of disinformation and misinformation, can delay progress in achieving greater climate security."

A fundamental challenge to progress in both climate change policy and solution implementation is a concern over how such policies and solutions might compete with other national security priorities. Dynamics in the national and international security space such as the COVID-19 pandemic, 'great power' competition with other nation states, and the rise of domestic terrorism, as well as the spread of disinformation and misinformation, at times can delay progress in achieving greater climate security.
The United States has made important progress in climate policy in recent years, but it still fails to take the necessary leadership in facilitating change. While the 2015 National Security Strategy outlined goals and actions that include significant immediate environmental impacts of climate change, strategies to date do not address the negative consequences on individual groups of people. Understanding the human impact is essential to effective future policies; this approach guides the recommendations presented later in this strategy. In addition, more dramatic changes that would effectively reduce emissions in the United States, like a carbon tax, remain widely debated and considered to be government overreach. Yet, climate change demands more significant action to protect U.S. national security interests.

The Biden Administration seeks to implement new climate policy to address the impact of climate change on national security more quickly. President Biden's plan for a clean energy revolution and environmental justice outlines ambitious goals such as reaching “a 100% clean energy economy and net-zero emissions no later than 2050.” The administration plans to achieve this by increasing spending in the climate sector in order to increase renewable energy use, such as wind and solar, as well as electric vehicle use. In addition, there are plans to work with the United States Environmental Protection Agency in order to cut methane and carbon emissions. Congress has demonstrated interest in intersectional climate change action that seeks to positively include communities of color and women to create more effective climate policy. This demonstrates critical support for the agenda outlined below.

The Connection Between Climate Change and Gender Equality
To understand the impact of climate change, the United States must look at those most affected: primarily, the global population of women. Because this is a global challenge with global repercussions, any strategy requires a global solution that should be aided by United States resources. Gender equality is critical in the discussion of climate change because the correlation between environment and gender is the key to finding long-term climate adaptation strategies. The disproportionate gendered impacts of climate change are particularly acute for women in low-income households globally. This is evidenced by recent data that reveals that an estimated “80 percent of studies find women are more likely to suffer from climate-driven food insecurity.” In 2021, climate-related events will prevent at least four million girls in low- and lower/middle-income countries from completing their education. Not only will women’s education be further imperiled, but the increasingly complex and fatal consequences of climate change exacerbate existing imbalanced statuses in society. For example, during natural disasters, the same shelters that provide human refuge trigger fear in women who are weary from domestic and sexual violence, and thus, often avoid using them altogether.
As the world shifts towards increasingly global interactions and influences, United States national security policies and strategies must mirror that transition. Through this National Girl Security Strategy, the United States aims to uplift women in such positions in order to reduce the effect of climate change and thus reduce the threat.

As climate situations become more dire, women are being forced to turn to different methods in order to secure some type of safety for both themselves and their families. Through such avenues, women's sexual and reproductive health (SRHR) are in peril. The uptick in natural disasters has also contributed to widespread healthcare access issues.

The recent White House National Strategy on Gender Equity and Equality emphasizes that “climate-related disasters hinder access to essential services, including sexual and reproductive health care.” In the United States, this was evident in the aftermath of the snowstorm that hit Texas in 2021, which impacted access for many of those seeking abortion care. After Hurricane Katrina struck New Orleans in 2005, researchers found that women faced higher rates of partner violence and sexual assault. Climate change and weather-related disasters also contribute to increases in child marriage rates as well as heightened interpersonal violence rates, as men use violence as a means to exert control over scarce natural resources.

Inclusive climate change solutions must include recognition and inclusion of Native and Indigenous populations as well. Due to a deep, historic relationship with ecosystems and habitats, Native and Indigenous women bring unparalleled knowledge to climate solutions. Furthermore, the Malala Fund estimates that combined action on girls' education and sexual and reproductive health and rights is the most cost-effective way to limit the global temperature rise to 2°C higher than pre-industrial levels by the end of the century. If every girl worldwide had access to twelve years of quality education, as well as reproductive healthcare and contraception, carbon emissions would be reduced by as much as 85.4 gigatons by 2050. This measure would be four times as effective as solar
power and the second-most effective solution for avoiding carbon emissions. Propositions that address women's needs, such as the Women and Climate Change Act of 2021 introduced in the House of Representatives in January 2021, detail how policies that are gender-sensitive are also more effective. The Women and Climate Change Act of 2021 states: "Women are shown to have a multiplier effect because women use their income and resources, when given the necessary tools, to increase the well-being of their children and families, and thus play a critical role in reducing food insecurity, poverty, and socioeconomic effects of climate change." Furthermore, this Act draws attention to other critical effects of climate change, including but not limited to: unpaid care work, access to education, access to reproductive health and rights, food insecurity, climate resilience, safety from gender-based violence, and women's involvement and leadership in the development of frameworks for climate resilience—all of which contribute to a nation's security.

**Priority Policy Actions**

As the world seeks to mitigate the challenges posed by climate change, the United States must not only see climate change as a threat, but also as an opportunity. The policy recommendations below emphasize the intersectionality of environmental protection, defense and national security, and social justice and equality. Developing holistic strategies that integrate these action areas will lead to more durable solutions to the climate crisis.

Going forward, climate policy must incorporate the following policy actions in order to be effective. The United States encourages collaboration with our global allies to fulfill these actions and ensure that climate change, a problem without passports or borders, is met with a global response.

**PRIORITY ACTION #1**

**Whole-of-Government Approach.** Incorporating a whole-of-government approach is essential to creating effective climate policies. The acute need for climate action and attention to environmental issues should be incorporated across sectors and government departments including the National Security community. For example, the United States Navy, Army, and Air Force each have a climate security advisory. On December 5, 2021, the Congressional policy 50 USC § 3060 went into effect, establishing a Climate Security Advisory Council for the purpose of "assisting intelligence analysts with respect to analysis community "is adequately prioritizing climate change." The United States should of climate security," facilitating relevant coordination, and ensuring that the intelligence community "is adequately prioritizing climate change." The United States should encourage continued progress towards integrating environmental analysis across agencies.

An example of applying the whole-of-government approach to connect climate change and other national security priorities relates to migration. In preparing for increased migration as sea levels begin to rise, the United States should employ a phased approach
to address the communities that are on the frontlines of the climate change crisis. There must be a push towards immigration resources such as career centers, access to education, housing, and health, for example, to facilitate a smooth process and demonstrate America’s leadership. Migration tears people and families away from their homes while also drastically altering the social and political landscapes of habitable land. There needs to be extensive diplomatic measures to develop a coordinated effort to address climate-induced mass forced migration that will be occurring.

PRIORITY ACTION #2

**Climate Change Educational Programs.** Through the establishment of a climate change curriculum, girls and all youth in the public education system would be taught the causes of climate change and its effects, but also ways in which to minimize its effects. This includes exposure to an expanded vision of green skills, which are the knowledge, abilities, values, and attitudes needed to live in, develop, and support a sustainable and resource-efficient society. This can be achieved by promoting sustainable values through climate education. The United States must start by implementing training institutions that prioritize core values to inform climate change curricula that can be shared with educators, by creating incentives for climate change education at the state-level or by integrating climate change education into existing science, technology, engineering, and math requirements through federal grants similar to Obama’s Race to the Top initiative.

Additionally, greater awareness around climate security, especially among younger generations, may spur community-based activism. Empowering students to take action in their respective schools ensures that policy and action will endure over time. This can also be encouraged by granting students excused absences in order to support student activism with federal policy. As a result, a high-level political declaration for the 2022 fiscal year would be effective in encouraging educational facilities to teach about climate change.

PRIORITY ACTION #3

**Elevating Marginalized Communities.** Economic advancement, women’s rights, and racial equality are also critical to effective climate policy. Important steps include:

- expanding access to and training for green jobs
- listening to the needs of marginalized communities who are disproportionately impacted by the changing climate and issues of pollution
- ensuring greater access to reproductive and maternal care services
- prioritizing funding towards the equality of ethnic and Indigenous minorities

The aforementioned areas of action, along with others that address the intersectionality between climate change and progress in other key areas, should guide interagency cooperation as well as relevant policies and programs.
In order make certain that climate security policies address the intersectional nature of the climate crisis and its disproportionate impacts on women and girls, the United States must ensure that each policy meets set standards for diversity, equity, inclusion, and accountability. In assessing whether or not policies meet these standards, the United States can draw inspiration from the Bechdel Test: a measure to determine whether media represents women in a three-dimensional manner by asking whether there are two or more named female characters in a film and whether they converse with each other about subjects other than men. With this in mind, it is strongly recommended that all climate security policies implemented by the United States meet at least half of the following measures of women's inclusion and empowerment:

1) The policy must include at least one clause specifically addressing its impact on women and girls and the way its implementation must consider this impact

2) The policy must include, or provide for, a gender analysis of its implications on women and girls domestically and internationally

3) The policymaking process must include at least 50 percent women in the climate security policymaking processes, and at least half of those women must be women of color (including Native and Indigenous women) to reflect population demographics in the United States

4) The policy must consider the importance of girls' education, including but not limited to: reproductive health education, climate change education etc.; if relevant, the policy should ensure it promotes access to education, or does not interfere with its completion

Furthermore, the United States must prioritize women's climate security initiatives and recognize the important contributions of women as experts, leaders, stakeholders, and educators, despite longstanding gender inequality.

"In assessing whether or not policies meet these standards, the United States can draw inspiration from the Bechdel Test: a measure to determine whether media represents women in a three-dimensional manner by asking whether there are two or more named female characters in a film and whether they converse with each other about subjects other than men."
Allocation of Resources. The United States has a unique role and ability to reprioritize its fiscal resources to address dire climate change challenges:

1) Diplomacy: Undoubtedly, the United States' involvement in wars and as a supplier of weapons and manpower to other countries has led to greater food insecurity, increased destruction, nuclear fall out, and other factors that worsen infrastructure and exacerbate the effects of climate change. By employing greater diplomatic efforts that consider the importance of international cooperation and climate action, the United States can work to mitigate the dire effects of war.

2) Budgeting: the United States should divert funding from its defense budget toward climate change efforts and initiatives that support those most directly affected by climate change in a way that promotes enduring self-sufficiency. Such shifts might mitigate the effects of climate change that spur further military intervention and have positive long-term effects, such as less extreme weather.\textsuperscript{19}

3) Unused resources: repurposing old aircraft models and other such devices to help deliver materials and resources would be a beneficial and sustainable alternative to scrapping and disposing of technology in a way that contributes to pollution.

4) Defense: The Department of Defense is the world's largest institutional user of petroleum and correspondingly, the single largest producer of greenhouse gasses (GHG) in the world. Furthermore, the United States military emits more CO2 than many other nation, including Morocco, Sweden, New Zealand, and Switzerland.\textsuperscript{20} If the Department of Defense were a country, the Pentagon would be the world's 55th largest CO2 emitter.\textsuperscript{21}

The military’s dependence on fossil fuels is also a threat to overseas operations; planes, ships, and vehicles can be placed in vulnerable positions when they refuel, with fuel convoys remaining notable targets for improvised explosive devices and other attacks.\textsuperscript{22} Statistics from the Department of Defense and the Energy Information Administration indicate that one American life is lost for every 24 fuel resupply missions.

With these factors in mind, the United States must be conscious of the environmental and security impacts of military deployment and seek to transition its military operations to renewable energy systems by 2050 or earlier. Potential initiatives to fulfill this goal include using alternative fuels like biofuel blends to power vehicles, implementing hybrid-electric propulsion technology in new aircraft models, and utilizing renewable energy microgrids to power facilities.\textsuperscript{23}
Military installations are also vulnerable with respect to climate change. According to the Department of Defense, approximately 1700 military bases on coastlines alone will be impacted by sea level rise.\textsuperscript{24} This type of large scale destruction that would come with further environmental consequences due to debris, abandoned structures, and construction of more bases. The United States should follow the example of the military bases already adapting to rising sea levels, such as Langley Air Force Base which has installed flood water pumps and built a shoreline seawall to protect its facilities. It is also vital that military building codes are revised to consider the impacts of climate change.\textsuperscript{25}

**Conclusion**

As the United States prioritizes national security concerns and reconciles competing priorities, it is important to regard climate change as a threat multiplier that not only exacerbates national security issues, but causes a host of other threats at the micro and macro level. Climate change is a consequential and bipartisan national security concern. Furthermore, it is an issue of equity and justice that disproportionately impacts women and historically marginalized communities. The authors of this strategy urge the United States and congressional leaders to collaborate with both existing partners and allies in mitigating climate change, while amplifying and respecting the voices of those most impacted by the climate crisis.
B. PROMOTING A WHOLE-OF-SOCIETY APPROACH TO CYBERSECURITY

“Cybersecurity education is essential for the foundations of a secure and successful future.”

Amanda Kay (Age: 17), Amulya Panakam (Age: 17), Sarah Velez (Age: 18), Sravya Kotamraju (Age: 16), and Zayna Cheema (Age: 15)

Technology now permeates every aspect of daily life in the United States. Over the past decade, there has been increasing concern over a workforce shortage in the Science, Technology, Engineering, and Mathematics (“STEM”) fields. The COVID-19 pandemic has fostered a digital transformation, with an unprecedented number of schools and businesses using virtual platforms for education, business, and more.²⁶ The pandemic highlighted the shortage of talent in technology and exposed pervasive cybersecurity threats to the United States.

The United States faces a multitude of cyberattacks from various groups and nations, which highlights the need for cybersecurity advancements in both the public and private sectors. Calls for greater diversity in cybersecurity teams to confront our most pressing cybersecurity challenges continue to gain momentum. Despite awareness of the importance of diversity in technology fields, cybersecurity has remained male-dominated as girls and minorities are typically discouraged from math and science at an early age.²⁷ The United States cannot prevent or respond to cybersecurity challenges unless it understands the risk and financial impact of ignoring the demand for cyber-literate professionals alongside the diffusive impacts cyber has on all citizens.

In addition, cyber hygiene is every citizen’s responsibility. As schools moved online due to the COVID-19 pandemic, cybersecurity became increasingly pertinent for schools, parents, and students due to a growing reliance on computers and other technologies. As the pandemic progressed, schools faced the issue of making sure that students were prepared for full-time online learning. Students needed access to computers, high-speed internet, and other resources that were not always necessary in the classroom. Cybersecurity education is essential for the foundations of a secure and successful future.

A more secure and prosperous future must also recognize the unique impacts of cybersecurity on disadvantaged regions in the United States, many of which are not able to offer cybersecurity education for the youth and do not have access to enough technology for all of their students, with ratios of economically-struggling students to computers being disproportionately high.²⁸ There are even other regions that have very high-poverty schools that have little to no access to the internet or technology as well. In
fact, almost 20 percent of households in the United States earn an annual income of $25,000 dollars or less, which may not afford basic needs nor technology-centered needs. This will negatively impact their exposure to education as the focus of these families will be more on immediate necessities. Students who are financially struggling or do not have access to technology are severely disadvantaged in their ability to learn about computer science and cybersecurity, such as coding, networking, and how to protect themselves online. Without any hands-on learning, underprivileged students are unable to receive proper education on this matter. Thus, it is imperative that the United States incentivize implementing cybersecurity and computer education to financially struggling regions.

Priority Policy Actions

PRIORITY ACTION #1

Creating a Cybersecurity Curriculum for Technology Throughout all Schools in the United States. The transition to online learning demonstrated the disparity between locations and students that had greater access to technology to those that did not. It directly correlates to cybersecurity education as computers, hard drives, and other technologies are necessary to attain a proper cybersecurity education.

While the US Department of Education (DOE) and the National Science Foundation (NSF) publish recommended teaching strategies for school districts, local governments may adopt or ignore these recommendations. This results in a diminished appreciation of and demand for technical classes. Inability to access these resources impedes students' ability to learn more about cybersecurity firsthand. Access to technology fosters equity in schools and a student's cybersecurity education both in and out of the classroom. Every student learns differently and technology provides even more opportunities for students to learn at a pace that is most suitable for them and their learning needs. Creating a space where both girls and minorities have access to computers to safely learn about cybersecurity would increase girls' and minorities' participation in computer classes while enhancing their cybersecurity education. Providing technology for all students and designing computer courses is critical to this education and promotes a more nuanced understanding of cybersecurity. A United States cyber education initiative will also cultivate a more secure and prepared nation to effectively confront various cybersecurity issues or threats against the United States.

PRIORITY ACTION #2

Incentivizing Cybersecurity As a Core Class. In order to prepare for the security challenges of our increasingly interconnected and technologically advanced societies, schools must start placing an emphasis on including cybersecurity and technical classes that promote online data security as core classes. Since courses and graduation eligibility are mainly
influenced by state and local governments, this causes a great amount of variation regarding what each area considers “critical” in a child's academic journey. However, the federal government still has an important role to play in education through its distribution of funding under the Every Student Succeeds Act (ESSA) and assistance programs for children with disabilities.

There have been efforts made to incentivize technology classes, like the Department of Homeland Security's (DHS) Cybersecurity Education and Training Assistance Program which distributes free cybersecurity, computer science, and STEM curriculum to K-12 educators. The limited funding in the education sector adds a challenge to integrating the proposed cybersecurity programs. This is compounded by the impact of prolonged exposure to technology on children. Online use must be managed for the protection of vulnerable individuals through the implementation of cybersecurity education and web monitoring practices used throughout national security. Even so, access to cybersecurity knowledge in American public schools forms a larger concern over America's future ability to protect from the increasing number of cyber threats. Incentives and the redirection of cybersecurity education are a key step in motivating schools to place a greater emphasis on cybersecurity education.

**Access to cybersecurity knowledge in American public schools forms a larger concern over America's future ability to protect from the increasing number of cyber threats.**

**PRIORITY ACTION #3**

**Implementing/Incentivizing Cybersecurity Programs in Public Schools.** Expanding federal education funding to include an incentive for those school districts that implement the numerous research and technical training strategies recommended by the DOE, NSF, and DHS would create a sense of importance for technical subjects, which are currently largely recognized as optional classes.

1) **Generate Local Grassroots Support.** In order to anticipate pushback by certain school districts, it is essential to generate local grassroots support to demonstrate the need for cybersecurity school programs. Additionally, working with local organizations will help transition such policy from a top-down regulation to a malleable approach informed by the needs of different communities.

2) **Providing Opportunities to Teachers.** Unlike previous efforts in technology literacy training, the proposed policy centers around children in elementary and early middle school at the developmental age where such concepts remain most necessary. Teachers must have the opportunity to increase their knowledge in the subject and be compensated for their time.
In the United States, Title I, Part A (Title I) of the Elementary and Secondary Education Act, as amended by the Every Student Succeeds Act (ESEA) provides financial assistance to local educational agencies for children from low-income families to help ensure that all children meet challenging state academic standards.\textsuperscript{31} As such, the utilization of Title I policy and funds towards bridging the gap between cybersecurity and low-income students will economically benefit the United States and strengthen U.S national security. Students in underprivileged and high-poverty districts are unlikely to be exposed to cyber-security education, and Title I can help overcome this lack of access that hinders opportunities for often underrepresented students to be exposed to opportunities within cybersecurity.

The integration of tech literacy classes at the elementary and middle school levels poses unique opportunities and challenges. With a succinct understanding of the precautions, integrating cybersecurity as a core class and therefore incentivizing cybersecurity programs in public schools requires the former.

PRIORITY ACTION #4

\textit{Provide Disadvantaged Students Access to Technology and Cybersecurity Opportunities.} In order to further incentivize implementing cybersecurity education, the United States should provide broadband access and connected devices to disadvantaged students by increasing the government budget on financial aid to low-income families. This ensures that low-income families and disadvantaged schools can receive sufficient financial aid to be able to afford critical cyber infrastructure.
In order for students to have hands-on-learning for cybersecurity, having stable connections to the internet as well as broadband access is necessary. The Federal Communications Commission has been working on this issue by creating the Emergency Broadband Benefit Program. The Emergency Broadband Benefit Program was created to assist families and households who are struggling to afford internet service during the COVID-19 pandemic. This program connects eligible households to jobs, healthcare services, virtual classrooms and more. The Emergency Broadband Benefit Program was recently replaced by Affordable Connectivity Program. The Affordable Connectivity Program was provided $14.2 billion by the Infrastructure Act, and the program provides eligible, disadvantaged households with a discount on broadband services and connected devices. Increasing funding and support from the Department of Education for this program will help enable the United States to provide cybersecurity education to disadvantaged students, bridge the digital divide in U.S. schools, and address inequities within cybersecurity education.

Conclusion
Through the revitalization of cyber education in the United States, underserved communities have opportunities to enter a dominating technology industry that is searching for talent. This creates the necessary groundwork to support marginalized populations, fulfill the shortage of workers in this field, and support and grow student endeavors in this industry. Implementing and incentivizing cybersecurity education can encourage school districts to emphasize cybersecurity education, allocate technology-based learning (to keep up with the digital transformation happening across all sectors), and initiate students to develop critical digital practices. Through cybersecurity education, disadvantaged students have increased access to technology. Ultimately, providing cybersecurity education will strengthen U.S. national security by preparing the future workforce, supporting preventative measures, and informing future generations to be digitally literate to create a cyber resilient America.
C. ACKNOWLEDGE THE PERVERSIVE IMPACTS OF GENDER-BASED VIOLENCE ON NATIONAL SECURITY

“Human trafficking is a violent crime and public health issue that violates human rights.”

Abby Tupper (Age: 17), Ashika Srivastava (Age: 18), Gurman Dhaliwal (Age: 19), Kenatu Habetaslassa (Age: 19), and Zikora Akanegbu (Age: 16)

Human trafficking is a violent crime and public health issue that violates human rights. In the United States, human trafficking disproportionally affects Native American and indigenous communities, yet the issue receives minimal attention. Native Americans are victimized by human trafficking at rates higher than that of the general population. In fact, Native American women are stalked more than twice the rate of other women and murdered at more than ten times the national average. Native Americans are already considered a vulnerable population because they experience higher levels of poverty and entry into the foster system, which are both risk factors for human trafficking.

The United States is failing to protect this vulnerable population and if unaddressed, this national security issue contributes heavily to international human trafficking that fuels conflict. In order to tackle this comprehensively, the United States must provide a multifaceted approach on the tribal, state, and federal level. Such a strategy should be created with an intersectional lens, explicitly include race in datasets to establish the true magnitude of human trafficking on specific populations, establish preventative measures to address complicit institutions, and include Native American and indigenous communities as active contributors in the creation, implementation, and enforcement of legislation.

The State of Gender-Based Violence
The UN Refugee Agency defines gender-based violence (GBV) as harmful acts directed at an individual based on their gender, rooted in the abuse of power and harmful gender norms. Sex trafficking is the epitome of gender-based violence. Yet, the issue has lacked awareness and direction of resources, likely because many of the victims belong to marginalized communities in the United States. Despite constituting nearly half of the victims in the United States, Native and indigenous women are often overlooked and left without proper support.

The current administration aims to prioritize the safety of Native American women because they experience higher rates of gender-based violence compared to the national average. Although the current stance is commendable, it must be noted that the history of the United States and Native American communities is marred by violence, subjugation,
and distrust. Numerous treaties (often utilizing offensive language) were broken, thereby eroding trust. The establishment of Indian Affairs within the Department of War in 1824 solidified the hostile attitude and contentious relationship between the United States and Native Americans. Today this hostile relationship is apparent in several facets of Native and indigenous life, including higher unemployment rates, lower household incomes, lack of medical care, shorter life expectancy, and a legal loophole that impedes accountability for crimes against girls and women.

With respect to human trafficking, an estimated 40 percent of women who are victims of sex trafficking identify as American Indian, Alaska Native, or First Nations. The high rate of poverty, historical trauma, homelessness, exposure to violence, and drug and alcohol abuse have created vulnerable conditions for Native and indigenous communities, making them targets for traffickers. Further, Native American women are raped 34.1 percent more than non-Native women, and 1 in 3 women will be raped in their lifetime. Importantly, it must be acknowledged that non-Indians commit 88 percent of violent crimes against Native American women.

There are a variety of contributors to this problem such as the fracking industry. “Man camps,” also referred to as “work-camp modular housing,” established to house fracking workers in remote areas of Minnesota, North Dakota, and South Dakota have created a high demand for sex in areas with drugs, alcohol, and limited supervision. Casinos also contributed to the demand for sex trafficking in these areas. The prevalence of sex trafficking of Native Americans is not solely based on the multiple risk factors associated with the community; as experts have explained, it is “a continuation of the marginalization of Native populations in the United States.” Native women have been fetishized, bought, sold, and traded since initial European colonization of the American continent.

**Human Trafficking Today**

The U.S State Department and International Labor Organization estimate that human trafficking is a $150 billion annual business profiting those in sex trafficking. It is estimated that sex trafficking is quickly exceeding other high-profit crimes such as narcotics and firearms, which may only exacerbate the problem. Current legislation, mostly protecting and assisting victims, is inadequate for addressing human trafficking. While human trafficking may not appear as a national security issue, it must be noted that where there is human trafficking, there is often human smuggling. Human smuggling is defined as “the movement of a person across a border.” Therefore, in order to prevent vulnerable populations from becoming a part of illegal human trafficking schemes, the United States must take steps to ensure that groups – including Native Americans – are provided protection. In summary, 25 million people are annually trafficked worldwide and human trafficking enables terrorist and armed groups, finances criminal organizations, and supports abusive regimes. This illustrates that by addressing human trafficking targeted
towards Native and indigenous communities, the United States can mitigate a global issue by stopping the supply of revenue and power for extremist groups.

Additionally, the lack of data on the issue makes it difficult for government agencies to understand its magnitude. According to Jordan Daniel, Founder & Executive Director of the Indigenous-led grassroots group Rising Hearts, “Indigenous and native women are very much exploited. But at the same time, we are continuously erased and invisible, in the greater public when knowing about how prevalent this violence is within our communities, not just on reservations, but in urban and rural settings.”

Out of the four federal agencies with portfolios that include sex trafficking, only one reports the race and ethnicity of the indigenous victims. Jurisdictional issues between state, tribal, and federal governments allow perpetrators to slip through the cracks because of poor communication between agencies. Non-native people cannot be arrested or prosecuted by tribes, they fall under federal jurisdiction, allowing traffickers to operate with little risk of getting caught. In addition, there is a gross lack of support services for at-risk individuals and rape survivors. Over two-thirds of the 650 tribal lands reported lack of sexual assault examiners and sexual assault response team programs: 381 reported no services within an hour driving distance.

If the United States does not effectively engage with this issue, it will contribute to a growing human trafficking and smuggling industry that undermines national and international security. Human trafficking can fuel conflict because it functions as a source of revenue and power for extremist groups. It also destabilizes communities, thereby amplifying conflict and suppressing development missions. Examples include Africa’s Lord’s Resistance Army, Libyan militias, the Islamic State, and Boko Haram who have all engaged in sex trafficking to force their victims to serve as combatants, messengers, cooks, spies, and attract and mobilize male fighters. If not addressed, human trafficking - specifically sex trafficking - perpetuates a cycle of poverty that leaves communities vulnerable to conflict instigated by extreme actors.

"If the United States does not effectively engage with this issue, it will contribute to a growing human trafficking and smuggling industry that undermines national and international security. Human trafficking can fuel conflict because it functions as a source of revenue and power for extremist groups. It also destabilizes communities, thereby amplifying conflict and suppressing development missions."
Priority Policy Actions

PRIORITY ACTION #1
Incorporate an Intersectional Lens Approach. According to the Oxford English Dictionary, the term “intersectionality” means “the interconnected nature of social categorizations such as race, class, and gender, regarded as creating overlapping and interdependent systems of discrimination or disadvantage.” It was coined in 1989 by professor Kimberlé Crenshaw to describe how race, class, gender, and other individual characteristics “intersect” with one another and inform one’s resulting relationship to power and privilege. In South Dakota, Native American women represent 40 percent of sex trafficking victims, though Native Americans make up only 8 percent of the state population. Without an intersectional lens, efforts to address inequalities and injustice in society, notably human trafficking, are likely to end up perpetuating systems of oppression.

PRIORITY ACTION #2
Include Race as a Factor for Victims in Federal Agency Datasets. One of the unique challenges faced by the Native American community in regard to human trafficking is that 3 out of 4 federal agencies that handle human trafficking cases disregard the ethnicity of the victim. This critical oversight prevents agencies from using aggregate data to report the true magnitude of human trafficking on specific populations. Without supporting statistics from appropriate federal agencies, Native American communities fail to receive appropriate resources and awareness to combat human trafficking. Therefore, the United States must include race as a factor for all human trafficking victims in all relevant federal agencies. This information can be used to highlight the disproportionate impact the Native American community faces from human trafficking and better understand potential solutions. This information will facilitate more awareness and direct more resources to the Native American communities.

PRIORITY ACTION #3
Focus on Contributors through Preventative Measures, not just on Victims. In addition, the United States should pursue preventative policy measures that would help ensure that the United States is targeting the perpetrators and consumers in this industry. As previously stated, there are many industries that are fueling the forced sex trafficking of Native women. The United States should institute a bureau within an agency that will investigate such industries' involvement in the creation of such camps and create measures that punish those involved. The United States must also work with industry to build stronger industry standards that hold accountable and prevent employee involvement in these illicit activities. With these measures in place, there will be a more hostile environment that will reduce traffickers' profit and help reduce the market incentive and potential harm faced by vulnerable populations. Finally, more public education and awareness is required so that when observed these traffickers can be reported to the proper authorities.
PRIORITY ACTION #4
Path Forward to Address Loophole. For a long period of time, Native American and indigenous tribes did not hold tribal jurisdiction over various non-Native violent crime offenders that committed these crimes on native reservations. This is one of many “jurisdictional loopholes” restricting the judicial power of Native and indigenous communities in cases of destructive and violent crimes committed on their own land. On March 7, 2013, former President Barack Obama signed the Violence Against Women Reauthorization Act (VAWA) of 2013 into law which allowed native and indigenous tribes to exercise "special domestic violence criminal jurisdiction" over offenders of domestic or dating violence on native and indigenous land. However, the scope of this law as applied to domestic violence crimes is limited and is not required for all tribes to follow. The United States must continue to consider how best to amend this law to cover a wider range of crimes and push for its adoption by all tribes. Currently, a bipartisan group of senators is working on a framework to update and reauthorize the VAWA list of crimes resulting in a firearm ban. Therefore, the United States should meet with various tribal leaders to discuss past and current issues regarding the law and to voice these concerns to members of the Senate in order to include these voices when advancing current and future legislation related to the VAWA.

Furthermore, native and indigenous women and girls are often hypersexualized and fetishized which leads to increased rates of sexual assault and murder. Examples of this are found in day-to-day media and culture including exaggerated Native American Halloween costumes and movies such as Pocahontas romanticize native and indigenous women. To combat this, the United States should focus on portraying more authentic women Native American role models and standards in mainstream American culture. This will increase accurate representation of native women and girls to educate and inform the public and decrease unrealistic expectations of native and indigenous women and girls. This effort may also reduce the “othering” of these vulnerable populations and result in increased awareness of the existing challenges faced by Native American populations.
Conclusion

The exploitation and devaluing of Native Americans has persisted since the colonizers came to America. Theft of Native land and the sexualization and illustration of Native Americans in the media has fostered a false narrative for decades and plagues the United States today. Violence against Native communities and the theft of their land in history has transformed into other means of exploitation and discrimination. Loopholes in the law and restricted mental health resources undermines these communities and makes them so vulnerable to human traffickers. The path forward must be a multifaceted approach with policies that include creating a safer environment and increased enforcement for Native Americans within the U.S. through tribal, state, and federal policies. Race and the role that it plays in policing and helping these disadvantaged communities needs to be at the forefront of public policy moving forward. Human trafficking cases need to represent race and the role that plays in the crime being committed. Education of the public should be a priority as well to change the conversation about Native American women and the hypersexualization and degradation forced on them. It is hoped that the enactment of these goals and policies will yield a safer, more just, and more equal America for Native and indigenous girls and women.
D. CONFRONTING THE RISE OF DOMESTIC TERRORISM

“Forming an advisory council of youth to educate policy makers on social media issues from those who use these platforms daily will ensure sustainability and longevity in combating this issue.”

Aimee Yan (Age: 19), Alexandra Rozmarin (Age: 17), Megan Mingo (Age: 19), Rachel Rochford (Age: 16), and Razel Suansing (Age: 19)

Following the January 6, 2021 attack on the Nation’s Capitol, the threat of domestic terrorism within the United States has grown. Concerns are exacerbated by an increasingly divisive political environment.

Partisanism and a divided government are not new features of democracy. For example, the bitter divide over slavery—prompted by regionalism and differing sources of economic revenue—resulted in over 600,000 deaths by the end of the Civil War. Even the undermining of democracy is derivative; the Bleeding Kansas events of the 1850s stem from disputes of voter fraud after the Kansas-Nebraska Act of 1854 decided new territories would decide their stances on slavery through popular sovereignty.57

The January 6th attack is only the most recent example of how partisan anger shakes the foundations of the “free world” and the pride it takes in autonomous governing. However, the rise of domestic terrorism predates 2021. In the past two years, the FBI reports that it has doubled its domestic terrorism caseload from about 1,000 to around 2,700 investigations.58 This rise is due to the impact of several variables, including the pervasive nature of technology and the breadth of communication and connectivity it enables, particularly on social media. The technological product development that has fundamentally changed the social fabric of the 21st century is now being used to enable homegrown terrorists in the United States.

Addressing Social Media as a New Front of Extremism

Experts point to five major themes to demonstrate how social media has catalyzed the process of extremism: the proliferation of echo chambers, more opportunities to be radicalized, radicalization acceleration, no physical constraints, and the opportunity for self-radicalization.59

Social Media Algorithms Create Echo Chambers of Extremist Content

Echo chambers are created by platforms such as Facebook and Twitter as a result of their confirmation algorithms. For instance, when Facebook changed its algorithm in 2018, it
shifted to an engagement-based ranking system, meaning content that people engage with—posts that receive larger numbers of reactions, comments and shares—is distributed more broadly. According to Facebook’s own internal research, “angry content” is more likely to engage the platform’s users. Consequently, users who frequently engage with “angry content” are more likely to be shown similar content in the future, creating an echo chamber in which other perspectives are not presented.

Instagram's infrastructure also breeds personalized echo chambers for users as its algorithm itself is reinforcing. A user clicking on one image will prompt more of that type of image to populate in features like the “Explore” page, especially with certain hashtags. Instagram also suggests that users follow additional accounts similar to those they already follow. In effect, someone who comes across extremist content is exposed to more and more of that content, creating a dangerous cycle. Instagram serves as an “entry” point for this type of content because of the algorithm’s speed in recommending similar content. Instagram combines the most dangerous aspects of other social media platforms: Facebook’s structure and Twitter’s youthful reach. Certain extremist social media accounts have huge followings; for example, @the_typical_liberal has over 2.5 million followers. Many of these social media accounts present the information in the form of memes with humor that disarms people, leaves them more susceptible to the ideas being conveyed, and minimizes the perceived harm these opinions create in the eyes of extremists. Also, Instagram relies on users to report problematic content, which is difficult to apply on a larger scale as a result of private accounts. People who follow the account believe in the ideas and do not report it; there is no outside policing force.

“Forming an advisory council of youth to educate policymakers on social media issues from those who use these platforms daily will ensure sustainability and longevity in combating this issue.”

Social Media’s Large Audience Fosters More Opportunities to Radicalize
Social media is widely used as a platform for recruitment to extremist causes. As of 2020, approximately 240 million Americans, or 72.3 percent of the American population were actively using social media each month. Social media has been widely used by terrorist groups, both foreign and domestic, for radicalization and recruitment purposes. In 2016, social media played a role in 90 percent of the extremists in Profiles of Individual Radicalization in the United States (PIRUS) data. Further, 73.2 percent of those included in the PIRUS data from 2011-2016 were using social media as a means of consuming extremist content.
Social media provides individuals with far more opportunities to radicalize, and with instant access to divisive content and people, this process is much more likely. Thus, one no longer needs to be in physical contact with another person to be radicalized: the process can be completed digitally. With these additional opportunities and without a need for physical contact, the process of radicalization has accelerated greatly. This acceleration is reflected in the number of domestic terror attacks in the United States. For instance, starting in 2017, the number of domestic-terror-related arrests began to outpace the number of international-terror-related arrests.65

**Instantaneous Nature of Social Media Contributes to Speed of Radicalization**

A major safeguard against disinformation, hate speech, obscenity, or other harmful content is the flagging of content. In an attempt to combat COVID-19 misinformation, Instagram rolled out a policy to attach a flag with a link to credible health sources on all COVID-19 content.66 In terms of political content, Facebook and Twitter have policies to flag content from politicians it deemed newsworthy enough to stay up but was false in some way.67 In a broader sense, these social media platforms have automated systems that flag potentially harmful content that violates policies to be taken down.

Both these types of flags—these are seen by users on content as well as flags that prompt companies to take down content—are a centerpiece in current policy makers' proposals for regulating harmful content. But, studies show that users disregard flags on content. For example, studies on flagged tweets from Former President Donald Trump that contain election misinformation found that tweets with a warning flag spread farther and for a longer period of time than unflagged tweets.68 Also, algorithm experts assert that a misunderstanding of the limitations of these flagging mechanisms limit their efficiency. These limitations include: one algorithm cannot be applied to a variety of domains; solely automated systems risk the disproportionate censorship of already censored groups as a result of internal biases; algorithms lack the clear definitions of unacceptable speech needed to accurately flag content; and human decision-making needs to always check automated systems’ work.69 Therefore, the speed at which radicalizing or extremist content is posted outpaces the abilities of these current mechanisms to keep the content in check.

**Social Media Circumvents Need for Physical Contact During Radicalization**

Social media happens primarily on the digital plane. Teenage girls will say that a contemporary stage of sleepovers resulting from the proliferation of social media is the “same-room-text-message-phase,” where despite being in the same room, conversation happens entirely through memes sent on social media platforms. Extremist organizations are no longer encumbered by the demands and costs of real-time organizing. Instead, organizations take advantage of online infrastructures to disseminate their messages. Although they can invest in online bots to further proliferate their message, studies found
that humans are most responsible for sharing misleading content as a result of its shock-factor.\textsuperscript{70}

As extremist groups take advantage of these online structures, digital literacy gaps leave older generations vulnerable. Multiple studies show that older adults, especially over 60, are most unable to identify disinformation as false. In fact, adults over 65 were seven times more likely than those under 29 to post articles from fake news domains.\textsuperscript{71} Therefore, although inequity is intrinsic to many avenues of American life, the digital landscape is steeped in it.

Self-Radicalization Possible through Prominence of Disinformation
A user’s experience on social media is self-driven. Thus, users engaging with false information on social media allows them to radicalize themselves or believe in the information enough that they seek out extremist causes.

An overarching theme is the prominence of disinformation on social media that often serves as radicalizing content. The proportion of online content that is “fake” or “real” is difficult to quantify because metrics are unreliable and the proliferation of non-human accounts could total over 40 percent of activity.\textsuperscript{72} Even so, disinformation was a driving force of the Capitol attack on January 6. Not only did a third of Republican representatives support a partisan audit of the election, but the court documents charging participants in the riot explain that beliefs in false narratives like widespread voter fraud prompted individuals to participate.\textsuperscript{73, 74} When people are constantly presented with a false view of the world, it does not take long for them to start accepting it. Experts call this a “post-
truth era,” where individuals are more likely to believe a piece of information if it fits into their existing world view, regardless of if it is true. Further, disinformation is often more engaging than the truth; one study found that falsehoods on Twitter were 70 percent more likely to be retweeted than the truth. Reducing the amount of disinformation on social media would decrease the amount of anger these sites create and thereby reduce their impact in the radicalization process.

Therefore, addressing the spread of disinformation on social media, the echo chamber it creates, the additional opportunities to radicalize and self-radicalize, the lack of physical contact required for radicalization, and the accelerated process created by social media will be essential in reducing the threat of domestic terrorism in the United States.

Priority Policy Actions

POLICY ACTION #1

*Requiring Redirection Algorithms to Combat Echo Chambers.* The main problem with current feed-creation algorithms is their lack of variability. Redirection algorithms are tech’s response to this problem and are currently being developed by Jigsaw, a unit under Google committed to combating disinformation, censorship, toxicity and violent extremism. The Redirect Method is an open-source program being developed by Google and Moonshot CVE that uses targeted ads to serve alternate perspectives to users searching for harmful content. This type of advertising does not fall under the category of bait-and-switch, where advertised content is completely different from actual content. Instead, certain searches trigger a variety of content instead of content reaffirming the original search. Therefore, users’ extremist views would be responded to and challenged, which is the most effective and empowering way to change a radical perspective. Although this program in particular was developed to counter ISIS messaging, it can be easily altered to counter American political misinformation.

POLICY ACTION #2

*Drafting a Public Forum Clause to Reduce Opportunities for Radicalization.* The creation of a “public forum clause” would directly combat the number of opportunities for radicalization. Such a clause would define social media networks with more than a certain number of monthly users as public forums, enabling further government regulation and public scrutiny. Because these networks impact the lives of so many people, they no longer fall strictly under the private sector but instead act as global institutions and require more transparency than they currently provide.
PRIORITY ACTION #3

Incentivizing Companies to Take Personal Responsibility to Reduce Speed of Proliferation of Information. Repealing sections of U.S. Code § 230 would remove protections for companies when harmful content is published on their sites, incentivizing them to introduce faster and more accurate mechanisms for taking down content, reducing the speed at which harmful information is spread. U.S. Code § 230 is a protection for private blocking and screening of offensive material. Subsection C1 of this code currently prevents internet service providers from being liable for the content published on their platforms. Policy makers currently struggle with incentivizing companies to take responsibility for content or terror plots occurring on their platforms, as these companies are motivated by growth and profit, and engagement with fear-mongering content sells. However, regulating these companies through laws and policies would provide a new motivation to invest resources into cultivating a safer platform free of harmful content.

PRIORITY ACTION #4

Advancing Nationwide Digital and Media Literacy Efforts and Creating an Advisory Council of Youth to Reduce Generational Gap. In order to disseminate the tools to spot and not fall victim to extremist content, the US government should fund both digital and media literacy efforts for both the new generation and the older ones. Implementing required curriculum in middle and high school that teaches students how to spot fake news is important. Further, funding curriculum to be taught at local libraries as well as community centers to help educate older generations on red flags on news articles will leave them less susceptible to disinformation attempts. Further, as mentioned above, efforts to regulate social media by policy makers are futile as a result of their lack of understanding of how social media operates on both a technical and practical level. Therefore, forming an advisory council of youth to educate policy makers on social media issues from those who use these platforms daily will ensure sustainability and longevity in combating this issue. As social media continues to transform in direct response to the needs of users, this advisory council will inform policy.

PRIORITY ACTION #5

Forming a Digital Counterterrorism Unit under Homeland Security to Disrupt Disinformation Plots. When terror plots are underway, the government should form a unit comprised of experts under Homeland Security dedicated to responding to and disrupting these plots. In this way, undue censorship is also prevented, as experts can determine threat levels. Because the problems these units will be fighting are domestic, this unit should fall under Homeland Security’s jurisdiction. Further, this unit could counter both physical organizations—such as another event like January 6—and digital fake news empires.
Conclusion
The role social media has played in furthering extremist causes is incredibly nuanced. Solutions which are implemented will have serious social and economic impacts and therefore must be carefully evaluated for their limitations. Consequently, this memo provides four immediately implementable solutions and three proposals which will require further consideration.

The three ideas for further consideration are as follows: creating a public forum clause in order to further regulate social media networks, repealing subsection C1 of U.S. Code § 230 - Protection for private blocking and screening of offensive material, and searching for positive incentives for social media networks to take greater responsibility for the content posted on their sites. The first two ideas are both rather complex and limited as they veer into legal and Constitutional considerations.

While considering the best ways to reduce radicalization on social media platforms, it is imperative that Constitutional freedoms, specifically First Amendment rights, are kept in mind. Additional regulation in these areas does enter that territory. Even on a Constitutional level, not all speech is protected. In cases where speech presents a "clear and present danger," speech can be restricted. In the case of domestic terrorism, this speech does present this type of danger, but that is at the end of the day up to the discretion of the courts. These actions will require extensive debate and planning before they are pursued.

The general solution to positively incentivizing social media networks to take responsibility for the content on their sites has stumped experts in implementation. The government is limited in its ability to offer or threaten these companies. Consequently, the best solution here would be one of social pressure. Just as the government needs to protect the welfare and well-being of citizens, these companies need to meet the needs and expectations of consumers. Creating a broader public understanding of the impacts of unregulated media networks is the most effective method of pressuring these companies into action while also respecting First Amendment rights and the rights of independent corporations as they are currently defined. Thus, the implementation of other more immediate solutions allows for progress while other avenues are explored.

The four immediate solutions are as follows: requiring redirection algorithms, improving digital and media literacy, creating a digital counterterrorism unit under the Department of Homeland Security, and creating a Youth Advisory Board to help implement these changes.

Redirection algorithms would be essential in reducing the echo chamber effects currently created by social media platforms. With the mass implementation of this software, those
most vulnerable to radicalization would be shown different perspectives rather than receiving constant variations of the same content.

Improving digital and media literacy will be essential in reducing radicalization on social media. In order to recognize the threat of disinformation on social media, individuals need to be able to recognize harmful or suspicious content. Improving these skills could definitely be worked on at school, but this is also an essential skill for older Americans and community programs with this goal would also be imperative.

A counterterrorism referral unit would allow the Department of Homeland Security to actively work to disarm disinformation plots. In this way, the department could take a more proactive role in combatting the online presence of domestic terror groups before it becomes a large issue, as opposed to afterward.

Finally, the implementation of a youth advisory board would allow for fresh perspectives on this issue. Youth are one of the more vulnerable groups for recruitment into domestic terror groups. Consequently, hearing from young people on how to best reduce the impact of these groups’ online presence would be highly beneficial.

Social media is a new phenomenon, bringing new challenges along with it. The use of these platforms for the purpose of recruitment into domestic terror groups is one of these unforeseen issues. However, with the implementation of these four solutions and consideration of the other three, radicalization through social media can be drastically reduced.
E. ADVANCING A MORE ETHICAL APPROACH TO ARTIFICIAL INTELLIGENCE AND NUCLEAR WEAPONS

“The United States should look beyond funding artificial intelligence defense projects and also fund American society’s understanding and integration of artificial intelligence in a broader sense.”

Ava Luna Pardo-Keegan (Age: 19), Ilyne Castellanos (Age: 20), Kristie Moore, (Age: 18), Mary Raines Alexander (Age: 17), and Sama Kubba (Age: 18)

As artificial intelligence and corresponding technologies emerge and integrate themselves into digital U.S. national security systems, it is increasingly evident that this progressive technology must be securely integrated across U.S. national security priorities. Current U.S. policy on the use of artificial intelligence in nuclear weapons enterprise and deployment is nonexistent, and while U.S. nuclear policy public dialogue often prioritizes North Korea and Iran, it is important to factor enabling technologies into a nuclear strategy.

Artificial intelligence is already prevalent across the nuclear technology domain. In an effort to minimize mechanical and human errors, artificial intelligence is integrated in the tactical, operational, and strategic levels of nuclear weapons, in command and control, advisory artificial intelligence that warns of nuclear weapon deployment by other states helps decision makers by yielding organizing data for faster, easier, and ideally more accurate decisions. This drastically helps human decision makers who confront information overload, compressed time, and stress in the moment of important nuclear decisions and has potential to reduce human error in safety protocols. Artificial intelligence is also used in missile defense warning systems and other systems. It is also being used to make nuclear targeting more accurate as the technology is trained to effectively follow moving objects. While early warning and data processing systems are helpful to quickly receive important alerts, over-reliance on this technology is subject to the risk of false reports and system failures. As artificial intelligence research and implementation continues to expand, the employment of the technology in nuclear weapons will only rise, requiring a policy to meet this need.

Moving forward, this strategy emphasizes the need for the secure development and integration of artificial intelligence in the operations of nuclear weapons. This point follows sophisticated advancements in nuclear weapon technology by China and Russia, whose progress aims to match, if not surpass, U.S. nuclear capabilities. In order to retain its position, support allies, and effectively deter and combat other nuclear states, the U.S.
needs to prioritize advancing the technological sophistication of its nuclear arsenal in a way that preserves strategic stability.

"Ultimately, everyone from civilians to scientists are stakeholders in policy and the implementation of artificial intelligence. Instilling a multi-stakeholder model of artificial intelligence is critical in creating technology that addresses ethical flaws such as racial biases that target marginalized communities, as well as system failures that compound others and result in extensive damage to public health, privacy, and safety."

Great power competition between the United States, China, and Russia politicizes nuclear technology and its potential use. The global rise of authoritarian China is a prime competitor to the United States' influence on all fronts of statehood: economic, political (domestically and abroad), cultural and military strength, stability and control. State-sponsored nuclear advancement alongside technological advancement in areas like artificial intelligence are just part of China’s expansive efforts. China's emergence has shifted the global power balance as it seeks to compete with the U.S. for economic and security purposes. On the other hand, Russia—an illiberal democracy—utilizes nuclear weapons as a political tool (in addition to and as an extension of its military capabilities) to leverage for greater global influence in negotiations.

The leaders of the great power competition will shape the new global order. A world led by the United States means that democratic values are prioritized as the shaping force of state regimes, their civil societies and international law and institutions in addition to norms around the integration and use of emerging technologies like artificial intelligence. China and Russia are states whose political structures and political legitimacy are founded in authoritarian values, an ideology which could craft a different world operating on fundamentally oppressive principles and prioritize economic gains in partnerships. It is not just the U.S. facing an existential crisis; the guarantee of civil liberties and livelihoods is also at stake. The United States must integrate artificial intelligence in its nuclear weapons technology to remain competitive with China and Russia. In addition to preserving
strategic defense, leading artificial intelligence integration in nuclear weapons gives the U.S. the opportunity to also lead in setting ethical norms and regulations around the practice.

China

Chinese military strategy emphasizes success in localized (to the Indo-Pacific), maritime conflicts through intelligence. At the moment, China lags behind the United States and Russia in nuclear forces capacity. China's arsenal includes 320 nuclear warheads, 90 nuclear capable intercontinental ballistic missiles, and numerous advanced nuclear weapons prototypes in development such as a H20 bomber—a supersonic aircraft bomber able to be equipped with conventional and nuclear missiles.

China's ambitious nuclear expansion program and its artificial intelligence deployment may be attributed to its fear of its nuclear weaknesses compared to U.S. nuclear capabilities. Robust nuclear forces are also seen as a political tool that would force the United States to cooperate in negotiations. Although China officially asserts a no-first-strike policy, experts more accurately describe China's goal as “assured retaliation” to possible U.S. attacks, mirroring U.S. nuclear development policy. It is also important to note Chinese military centralization of conventional and nuclear forces in supply and infrastructure. For example, Chinese nuclear submarines share communication channels with conventional submarines.

China has not only pursued growth in the use of artificial intelligence for their nuclear arsenal, but their investment in artificial intelligence has expanded in a variety of industries. Through their artificial intelligence expenditure, China has incorporated artificial intelligence systems into their financial technology, establishing them as the leader in digitized financial processes. For instance, in mobile payments in 2018, Chinese citizens were seen to spend in total about $19 trillion whereas American mobile payments fall under $1 trillion. Artificial intelligence dominance does not end with fintech, as China continues to lead in nearly all fields of artificial intelligence efficiency with the Chinese speechtech company iFlytek regularly surpassing American companies—Google, Microsoft, Facebook, etc—in system performance competitions between countries in English. With the rapid increase in domestic investment in the private sector, the artificial intelligence advancements that develop from systems such as WeChat and Tencent are further utilized in their weapons of mass destruction.

Considering China’s artificial intelligence advancement, it is necessary for the United States to invest to support domestic artificial intelligence advancement to protect U.S. national security. For example, the U.S. is largely dependent on artificial intelligence chips that could become irrelevant if out-paced by progressive Chinese technology, as Beijing pledges to “produce 70% of locally-used chips by 2025.” Advancement of Chinese chips
means enhanced capabilities in decision making, facial recognition systems, Chinese user interest assessments, and conventional military strategy that present security challenges to the U.S. With Chinese investments in artificial intelligence research and development surging past American standards, the U.S. lacks intellectual groundwork and hardware necessary to remain competitive with Chinese integration of artificial intelligence into nuclear weapons.87

To achieve the grand vision of matching U.S. nuclear capabilities, China has utilized its skills in “large-scale infrastructure and industrial manufacturing” to support its nuclear capabilities. China has also prioritized technological advancement in its nuclear weapons development program. Following the principle of intelligentized (智能化) warfare, China has looked to integrate artificial intelligence into its nuclear programming through autonomous decision-making, early-warning, guidance, and targeting systems optimized by machine learning. This is made possible by “military-civil fusion” (军民融合)—private and university joint efforts in development on artificial intelligence in nuclear forces.88

Meanwhile, although the U.S. government regularly sponsors public research, the United States must improve public-private partnerships to address challenges in utilizing private sector development for U.S. national security applications.

A recent successful test of a Chinese hypersonic glide vehicle with possible nuclear and missile space deployment capabilities highlighted the rapid advancement of Chinese technology. This new capability surprised U.S. national security experts, especially since the U.S. currently has no method of stopping attacks deployed by maneuvering space weapons and has failed glide attempts of its own.89 Such a weapon is especially concerning given US reliance on satellites in not just nuclear operations through nuclear command, control, and communications and early-warning capabilities but also in enabling technology in everyday American life.90

**Russia**

Since the end of the Cold War, the tense relationship between the U.S. and Russia has largely been shaped by lasting mistrust and the proliferation of new technologies and concern regarding weapons of mass destruction. Despite active treaties to deter conflict, technology developments have increased risks of miscommunication, miscalculation, and an arms race between the United States and Russia. In Putin's desire to retain relevance and regain the political, economic, and ideological prowess it once had, Russia has focused on building up its nuclear military capabilities. In doing so, Russia aims to make up for its lacking conventional capabilities. Russia has also pursued niche areas in which the country can advance dominance and gain a unique advantage over adversaries. This is particularly clear with Russia's interest in asymmetric warfare in the digital domain through artificial intelligence, which has already
directly impacted the United States. In addition, Russia’s development of more than 150 new artificial intelligence enabled military systems attests to the threat Russian capabilities pose to the United States and key allies in the region.⁹¹

Russia seeks to become a leader in artificial intelligence technology and has already begun to multiply artificial intelligence technology development with a focus on nuclear weapons. However, compared to the United States, Russia is behind in the field of artificial intelligence development and research, especially in the realm of nuclear warfare.⁹² Russia has been very clear about the intention to use artificial intelligence systems to enhance nuclear weapons. According to a recent report by East West Center, a think tank focused on analysis around United States, Asia, and Pacific, Russian innovations include: an artificial intelligence-equipped missile-carrying bomber, hypersonic glide vehicles for delivery of payloads, and a nuclear-powered underwater vehicle with artificial intelligence enabling it to be unmanned and still carry nuclear weapons.⁹³

Despite Russia’s continued efforts, the state continues to fall behind the United States, partly due to the research methodology. In the United States, artificial intelligence research and related projects are not only developed by the government but with the private sector.⁹⁴ Meanwhile, in Russia, almost all artificial intelligence research projects are government-funded; there is limited risk-prone private sector investment. In response to this deficiency, Russia has launched many new projects in artificial intelligence at the Skolkovo Innovation Hub with research clusters focused on nuclear weapons.⁹⁵

During the Defense Department’s artificial intelligence symposium this past summer, it was noted that Russia is quickly advancing its development of nuclear weapons with artificial intelligence and that it is important to understand that they are becoming a significant threat with artificial intelligence nuclear weapons in the near future.⁹⁶ Thus it is critical that the United States set robust standards and regulations for artificial intelligence in nuclear weapons.

**Priority Policy Actions**

**Priority Action #1**

*Adopt a Cohesive Stance on the Operational and Ethical Principles of Artificial Intelligence.* The United States must integrate artificial intelligence in operational applications such as early warning, steer away from artificial intelligence in launch authority and adopt a cohesive stance on operational and ethical principles regarding artificial intelligence in the U.S. Nuclear Posture Review, the U.S. Ballistic Missile Defense Review, and U.S. National Security Strategy. Such an integrated framework enables reassured engagement of
academics, practitioners and experts in the artificial intelligence and nuclear fields. The ethical values guiding the integration of artificial intelligence should include a lack of sole-dependence on certain artificial intelligence systems, creating resilience in the network and maintaining human involvement, and artificial intelligence systems should also be challenged with red-teaming, forcing differing approaches to be considered.

Ultimately, everyone from civilians to scientists are stakeholders in policy and the implementation of artificial intelligence. Instilling a multi-stakeholder model of artificial intelligence is critical in creating technology that addresses ethical flaws such as racial biases that target marginalized communities, as well as system failures that compound others and result in extensive damage to public health, privacy, and safety. Having diverse experts behind emerging policy and technology that includes women, people of color, and other groups that will most strongly face the brunt of failures is an ethical concern that must be addressed by the U.S.

Concurrently, the U.S. should encourage international discussions surrounding a nuclear weapons strategy. By working within international frameworks and negotiating new agreements regarding the development and use of artificial intelligence as it relates to weapons of mass destruction, the United States can prevent a Cold War-esque arms race. This can be done multilaterally within related UN bodies or through the negotiation of new treaties that build upon New START between Russia and the United States.

PRIORITY ACTION #2

*Increase Investment into Artificial Intelligence Research and Education.*

The United States must invest more money into artificial intelligence research, education, and application across the technology domain. The application of artificial intelligence in defense projects is merely a subset of a greater dialogue and more comprehensive understanding of artificial intelligence. The U.S. needs to take advantage of its strong academic and private business communities and commit funding to think tanks, public-private business partnerships, schools and universities, and other academic incubator programming on diverse uses of artificial intelligence to better understand and provoke creativity on its range of application, ethical considerations, accountability, and national security implications.

PRIORITY ACTION #3

*Support Track One and Track Two Dialogue About the Role of Artificial Intelligence.*

The United States must support track one, and consequently, track two dialogue about the role of artificial intelligence and other technological advancements in nuclear capabilities in international discussions with China and Russia. There should be a focus on dialogues with teams of policy makers, scientists, legal experts, ethical analysis experts and any relevant adjacent experts from each country to discuss the implications of artificial intelligence being
used in nuclear weapons. With a diverse group of experts, more perspectives and ideas can be covered as the topic of nuclear security with artificial intelligence is multidimensional. The United States should advocate for the prevention of artificial intelligence in command and control operations of nuclear weapons in multilateral discussions and set an international standard to support this norm.

It should be noted that the United States and Russia's nuclear arsenals compared to China will create challenges in diplomatic negotiations. A mechanism to enforce agreements is also a needed development as China and Russia should face consequences for not abiding by international regulations. In these meetings, representatives can also discuss strategic collaboration in areas of mutual interest or concern (ex. terrorism, space exploration, and nuclear safety).

PRIORITY ACTION #4

*Develop a More Agile U.S. Posture toward China and Russia.*

The United States should understand and consider Chinese and Russian military strategies and operational structures when tailoring its own nuclear defense strategy and seek opportunities to increase mutual understanding and provide clarification to prevent miscommunication and escalation. The centralization of Chinese command structure with conventional and nuclear forces can be a vulnerability in the necessary case of direct military confrontation. Russia is currently behind in artificial intelligence research and tactics in nuclear security compared to the United States which can also be used by U.S. intelligence for strategies. Otherwise, the U.S. should remain cognizant of this vulnerability and understand that an attack on conventional forces could lead to nuclear warfare if China or Russia feels threatened.

"The U.S. needs to invest in space military defense technology and training, but must also maintain space as a peaceful realm through diplomatic negotiations."

PRIORITY ACTION #5

*Advance Enhanced Protections for U.S. Satellites.*

The United States needs to bolden its protection of pre-existing nuclear infrastructure, specifically in space. Satellites are valuable and crucial to the U.S., both for their civilian and defense implications, particularly in enabling nuclear operations. With Chinese advancement in nuclear-capable space technology, the United States needs to take steps to protect its space infrastructure through both military development and diplomatic negotiations to create norms that preserve the peaceful use of space. The U.S. needs to invest in space military defense technology and training, but also must maintain space as a peaceful realm through diplomatic negotiations.
Notes (Climate Change)


9. Ibid.

Notes (Climate Change, Cont.)


13. Ibid.


19. When interviewed, Professor Nichola Minott of Boston College stressed that what needs to happen now is a shifting funding away from the most harmful expenses, such as fossil fuels, towards policies that emphasize and support renewable energy and energy saving technologies.


Notes (Cybersecurity)

26. COVID-19’s impact on American industries and businesses:
https://www.forbes.com/sites/larryenglish/2021/06/01/the-tech-talent-war-has-no-end-in-sight-heres-what-you-need-to-know/?sh=46a556d05f2d


28. Statistics on student to computer ratio and internet access in disadvantaged regions:
https://www.ets.org/Media/Research/pdf/PICCOMPCLSS.pdf

29. Statistics on United States households’ annual incomes:

30. CETAP grant and programs:
Cybersecurity in the Classroom | National Initiative for Cybersecurity Careers and Studies (cisa.gov)

31. Improving BASIC programs operated by local educational agencies (ESEA Title I, part A). Office of Elementary and Secondary Education. (2020, November 5).


Notes (Gender-Based Violence)


Notes (Gender-Based Violence, Cont.)


47. Daniels, Jordan Marie. Interview by Ashika Srivastava


49. Ibid., 34.


52. Demarginalizing the intersection of race and sex: A black ... (n.d.). https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1052&context=uclf


Notes (Domestic Terrorism)


Notes (Artificial Intelligence)


82. Ibid Brown, “Understanding the Risks.”


84. Ibid Allison, “Is China Beating Us?”

85. Ibid Allison, “Is China Beating Us?”


87. Ibid Allison, “Is China Beating Us?”


90. Ibid Brown, “Understanding the Risks.”


Notes (Artificial Intelligence, Cont.)


96. Ibid Tadjeh.